AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: s/Tiffany Edgmon 11/01/2024

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNTS WITH UNIQUE IDENTIFICATION NUMBERS: 100088501780416

Case No. M-24- 822-STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Material Containing Child Pornography

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

David A Garrison SA FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: Nov 1, 2024

Judge's signature

City and state: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David Garrison, Special Agent with the Federal Bureau of Investigation ("FBI"), Oklahoma City, Oklahoma, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI since June of 2005 and have been assigned to the Oklahoma City FBI Field Office since January of 2013. During that time, I have conducted a wide variety of investigations, including cases involving child pornography and sexual exploitation of children.

2. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The information contained in this Affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and review of documents and records. This Affidavit is made in support of an application for a warrant to search information associated with a certain Facebook account, 100088501780416, (herein after referred to as the "**SUBJECT ACCOUNT**") that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), a company headquartered in Menlo Park, California, as further described herein and in Attachment A, for the items specified in Attachment B hereto, which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. § 2252A.

4. This investigation, described more fully below, has revealed that an individual knowingly utilized the BitTorrent peer-to-peer ("P2P") file-sharing network from 5309 NW 45th Street, Warr Acres, Oklahoma (herein after referred to as the RESIDENCE), to possess and distribute child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2), and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations

are located on the **SUBJECT ACCOUNT**.

5. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

TERMS

6. Based on my training and experience, I use the following technical terms and definitions:

a. An Internet Protocol ("IP") address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, or long-term, IP addresses. Other computers have dynamic, or frequently changing, IP addresses.

b. Single-source download applies to a file that is downloaded from one IP address only. In P2P software, users often download different parts of the same file from many other users at once in an attempt to gain the file quicker. A single-source download comes from one user/IP address instead.

BACKGROUND ON P2P FILE SHARING

7. A growing phenomenon on the Internet is P2P file sharing. P2P file-sharing software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together.

8. To access the P2P networks, a user first obtains the P2P software from the Internet. This software is used exclusively for the purpose of sharing digital files. In general, P2P software allows the user to set up file(s) on his/her computer so that the files can be shared with others running compatible P2P software. In essence, a user allows his/her computer to be searched and accessed by other users of the network. If another user finds a file of interest on his/her computer, the other user may download that file. A user obtains files by opening the P2P software on his/her computer and conducting keyword searches of the P2P network. The P2P software then conducts a search of all computers connected to that network to determine whether any files matching the search term(s) are currently being shared by any other user on that network.

9. BitTorrent, one type of P2P software, sets up its searches by keywords, typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the actual files being shared, only the file referred to as a ".torrent" file. The user then selects one or more .torrent files from the results for download. The .torrent files contain instructions on how a user can download the file(s) referenced in the torrent. The download of file(s) referenced by the .torrent file is achieved using a BitTorrent client/program, through a direct connection between the computer requesting the file(s) and the computer(s) sharing the actual file(s) (not the .torrent file but the actual files referenced in the .torrent file, using any BitTorrent client/program).

10. For example, a person interested in obtaining images of child pornography would open the BitTorrent website or program on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user then selects a .torrent from the results displayed. The .torrent file is the set of instructions a BitTorrent client/program needs to find the files referenced

in the .torrent file. Once the .torrent file is downloaded, it is used by a BitTorrent client/program, previously downloaded and installed by the user, to download the actual files. The actual file(s) are downloaded directly from the computer or computers sharing the file(s). The download is achieved via the Internet. The downloaded file(s) are then downloaded/stored in an area previously designated by the user and/or the software. The downloaded files will remain until moved or deleted.

11. A P2P file transfer is assisted by reference to an IP address, which provides a unique location making it possible for data to be transferred between computers. The computer running the file sharing application, in this case a BitTorrent application, has an IP address assigned to it while it is on the Internet. BitTorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them.

12. Law enforcement officers using BitTorrent log the IP address which has sent the files or information regarding files being shared. Investigators can then search public records, such as ARIN, that are available on the Internet to determine the Internet service provider who has assigned that particular IP address. Based upon the IP address, investigators can obtain subscriber information from the Internet service provider. The subscriber information identifies the individual to whom the Internet service account is registered.

13. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers/sources. The advantage of this is that it speeds up the time it takes to download the file. However, software used by the FBI to download files from P2P networks will only download from

a single source, via a direct connection (i.e., a single source download).

14. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person who shares child pornography files on a P2P network is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography.

15. Even though the P2P network links together computers from all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is specifically designed to only allow the download of files that have been selected. A user does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

BACKGROUND OF INVESTIGATION

16. This case originated on August 26, 2024, when law enforcement conducted an online undercover investigation to identify individuals possessing and sharing child pornography from July 25, 2024, August 5, 2024, and August 25, 2024, on the Internet using the BitTorrent P2P network. Law enforcement used a P2P file-sharing program that utilizes a single-source download process. Based upon my training and experience, I was familiar with P2P file-sharing, specifically the operation of the BitTorrent network. Law enforcement directed their focus to a computer using IP address 68.97.174.205 because, on July 25, 2024, it was associated with a torrent file that referenced two files, at least one of which had been identified as a file of interest in child pornography investigations.

17. On August 5, 2024, between 6:17 p.m. and 6:30 p.m., Central Daylight Savings

Time, law enforcement completed single-source downloads of approximately two files that the device using IP address 68.97.174.205 was making available for others to download on the BitTorrent network. Each of the files was downloaded directly from the device using IP address 68.97.174.205. Based upon my training and experience, I determined one of the files depicted children under the age of eighteen years engaged in lascivious exhibitions of the genitals, and sexually explicit conduct, that constitutes child pornography as defined by 18 U.S.C. § 2256. One of these files are described below:

a. Filename: pedomom.mp4
Description: A portion of this video depicts an adult female, with red fingernail polish, performing oral sex on a male toddler who is laying on his back. The female is wearing a mask that covers her face but exposes her eyes. The length of the video was 3 minutes and 53 seconds.

18. Between August 25, 2024, at approximately 8:12 p.m., and August 26, 2024, at approximately 7:51 a.m., Central Daylight Savings Time, law enforcement completed single-source downloads of approximately ten files that the device using IP address 68.97.174.205 was making available for others to download on the BitTorrent network. Each of the files was downloaded directly from the device using IP address 68.97.174.205. Based upon my training and experience, I determined several of these files depict children under the age of eighteen years engaged in lascivious exhibitions of the genitals, and sexually explicit conduct, that constitutes child pornography as defined by 18 U.S.C. § 2256. One of these files are described below:

a. Filename: 00303.mp4
Description: The video depicts a prepubescent female, with no clothes on below her waist while sitting on a bed, performing oral sex on a male. She pulls her mouth away at one point and the male places his hand on the back of her head and holds her head while she continues to perform oral sex. Towards the end of the video, the prepubescent female puts her hands on her face and lays back onto the bed. The length of the video is 39 seconds.

19. Law enforcement determined that Cox Communications, Inc. was the Internet

service provider for IP address 5309 NW 45th Street, Warr Acres, Oklahoma 73122. Pursuant to administrative subpoenas issued on August 7, 2024, Cox Communications, Inc. provided the following Internet subscriber information for the IP address 68.97.174.205 for the July 25 and August 5 downloads as described above[1]:

Name:	Dawn Weeks
Address:	5309 NW 45th Street, Warr Acres, Oklahoma 73122
Phone Numbers:	405-787-2105 405-808-6782

20. On September 17, 2024, a search warrant was executed at the RESIDENCE. During the course of the search and on-site preview of digital devices, no evidence of violations of 18 U.S.C. § 2252A was found. Additionally, during separate interviews, Dawn Weeks (Dawn) and her husband, Richard Weeks (Richard), disclosed individuals later identified as Brendon Shea Cooper (Cooper) and Katy Raeann Hale (Hale) resided at and near the RESIDENCE from approximately September of 2023 to July of 2024.

21. On September 17, 2024, I conducted an additional telephonic interview with Dawn who described how Cooper and Hale spent time at the RESIDENCE as indicated, but, following Dawn and Richard contracting Covid 19 around August 26-27, 2024, they have not spent as much time as previously. The last captured download of child pornography at the RESIDENCE was August 26, 2024.

22. Due to an outstanding warrant for Cooper and drug paraphernalia charges, on September 17, 2024, Cooper and Hale were arrested by officers from the Warr Acres Police Department while sitting in a vehicle near the RESIDENCE.[2] At the time of their arrest, cell phones

[1] The results for the administrative subpoena to Cox Communications Inc. for the August 25-26, 2024 downloads is pending. It is anticipated the subscriber results will be the same as the previous subpoena returns.
[2] Officers with the Warr Acres Police Department located drug paraphernalia in the vehicle.

were in the control of or nearby both Cooper and Hale. Specifically, a black phone (black phone) was seized from the back passenger seat and a blue Motorola phone (Motorola) from the front passenger seat occupied by Hale. An additional TCL smart phone (TCL) was seized from Cooper's hand while sitting in the front driver's seat at the time of his arrest. All of the devices were collected by the Warr Acres Police Department and checked into their evidence control.

23. During the course of the search warrant at the RESIDENCE, the router was examined and its' log history was accessed revealing a number of MAC addresses[3] which utilized the router to gain access to the internet via the assigned IP address. On September 18, 2024, a search warrant was executed on the TCL, and the other devices, to determine if the MAC Addresses assigned to these devices were listed among the MAC Addresses displayed by the examined router. An examination of the black phone and Motorola revealed MAC Addresses that matched MAC Addresses found within the router log history, indicating they accessed the internet utilizing the assigned IP address and network located at the RESIDENCE. The MAC Address of the TCL did not match the listed MAC addresses contained within the RESIDENCE's router log history.

24. A subsequent search warrant was executed on the black phone and the Motorola. A forensic examination of the black phone did not reveal evidence related to the child pornography downloads associated with the RESIDENCE. The examination of the Motorola revealed three images containing child pornography as defined by 18 U.S.C. § 2256. Additionally, one of the images appeared to be a still frame from the video, "pedomom.mp4", described in paragraph 17a of this affidavit. The referenced video was downloaded on August 5, 2024, utilizing BitTorrent software via the IP address assigned to the RESIDENCE.

[3] A "MAC Address", or media access control address, is a unique identifier for a device on a network. It's a 12-digit hexadecimal number that's usually found on a device's network interface card.

25. A further examination of the Motorola revealed downloading of both utorrent and bittorrent client applications in February and April of 2024, respectively, which match the type of software and applications utilized by the individual(s) responsible for the child pornography downloads at the RESIDENCE.

26. Based on the evidence contained within the Motorola, a subsequent search was conducted on the TCL cell phone. Texts between Cooper and Hale (extracted from native messages from the TCL phone) from December 21, 2022 (during which they discussed sexual role playing) included the following:

Cooper: I want to add something to the daddy and daughter Rp

Hale: What's that baby

Cooper: What big we add one of our girls to it not in real life but on here[4]

Cooper: Don't judge

Hale: Idk baby I don't want us to get caught and get in to trouble baby

Cooper: We won't baby I promise

Hale: But there is always that possibility though if the wrong person was to see

Cooper: Delete once you are done baby

Hale: As we we're doing it on here or our phone baby

Cooper: No one will see baby unless we just do it in real life which would be hot as well lol

Hale: No we ain't doing it in real life baby what would make you think I would feel ok with that. How about we just make up a random girls name instead baby

27. During a text exchange on January 9, 2023, Cooper and Hale discussed

[4] Hale has three prepubescent girls from a previous relationship.

incorporating one of Hale's juvenile daughters in their sexual activities. At one point of the exchange, Cooper stated, "Ok, so JANE DOE[5] has caught me naked with you and she has talked to me about it but she does want to start playing with us in bed and she wants to be played with too I have told her if that ever happened and she says anything to anyone me and you would get in trouble but she swears up and down she won't and I believe her so was going to see if she could sleep with us a night or two a week and us three have fun and see if we like it but I don't want you mad at me or her because I love you and respect you but I think it will be fun and I kinda want to does that make me a bad person baby"

28. A series of emails (ranging from December 8, 2022 to January 25, 2023) from notification@facebookmail.com (titled "Facebook Groups") to both an @groups.facebook.com Brendon Cooper email address and bornwicked420@gmail.com (which are addressed to "Brendon") verified membership in various Facebook Groups for Facebook account holder 100088501780416. The groups included: "Littles and Abdi Play Space"[6], "Incest Love", "DDLG centre"[7], "Mommies and Littles/Middles Safe Place 18+", "TEENS CLUB (joking) (13-21)", "CUTE KIDS AROUND THE WORLD", and "Secret Room".[8]

29. On December 22, 2022, the **SUBJECT ACCOUNT** received a message from a Facebook user for the group "Little café DDLG, MDLG, DDLB, MDLB, CG, PETS"[9]: "Anybody have discord and want to join a group for littles[10]".

---

[5] Hale's second oldest daughter who was nine years old at the time of this text exchange.
[6] This group caters to individuals who have fetishes involving "Adult Baby/Diaper Lover" and "Daddy Dom/Little Girl" roleplays.
[7] DDLG means "Daddy Dom/Little Girl"
[8] Facebook groups set to "private" or 'secret" allow only members to access and see the content.
[9] MDLG means "Mommy Dom/Little Girl", DDLB means "Daddy Dom/Little Boy", MDLB means "Mommy Dom/Little Boy", CG means "Caregiver" usually of someone acting as a "Little" or juvenile, PET can mean a submissive in a Dom/Sub relationship.
[10] Littles is a term used by individuals acting or conversing at an age younger than they truly are, usually as a minor.

30. Through my training and experience, it is common for individuals engaged in the downloading and storing of child pornography to move or transfer the material from one digital device to another, or from social media/instant messaging platforms to digital devices for ease of access. On November 1, 2024, in response to a subpoena for subscriber information for the **SUBJECT ACCOUNT** for the period of November 1, 2022 to March 1, 2023, returned information listing the subscribed user as Brendon Cooper.

BACKGROUND ON FACEBOOK AND META

31. Meta owns and operates Facebook, a free-access social networking website that can be accessed at http://www.facebook.com. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

32. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

33. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account

includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

34. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

35. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

36. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can "tag" other users in a photo or video, and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

37. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats. of the date of each call. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

38. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

39. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

40. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

41. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

42. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

43. In addition to the applications described above, Meta provides users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user

accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

44. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

45. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

46. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

47. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

48. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

SEARCHING COMPUTERS

49. Searching computers for criminal evidence is a highly technical process requiring skill and a properly controlled environment. The search of a computer or computer system is an exacting scientific procedure designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is vulnerable to tampering or destruction, the controlled atmosphere of a laboratory is essential to complete this task. The FBI, Oklahoma City Division ("OCD"), has such a laboratory staffed with certified computer forensic examiners. At least one certified forensic examiner will be present and take custody of any computers and storage media found at the search location. All magnetic storage media will be taken to the FBI OCD lab for analysis. Identical copies of the original storage media will be produced by the assigned forensic examiner so as to maintain the integrity of the original evidence. Due to the fact that child pornography is by its nature contraband, and illegal to possess, making an image of the computer's hard drive and other storage media on site is not a feasible alternative.

ADDITIONAL CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

50. The following indicates characteristics of child pornography collectors that I have learned through training, working multiple investigations involving child pornography, and from other law enforcement officers with a background in child pornography investigations:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer to peer, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from

which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location.

CONCLUSION

51. Based on the above information, and my training and experience, the user of the **SUBJECT ACCOUNT** is engaging in behavior indicative of an individual who has a sexual attraction to children and there is probable cause to believe that the foregoing laws have been violated, and that the property, evidence, fruits, and instrumentalities of these offenses are located on the **SUBJECT ACCOUNT.**

52. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

53. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is "a district court of the United States" with "jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

54. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the **SUBJECT ACCOUNT**, described in Attachment A, authorizing the seizure of the items described in Attachment B to this Affidavit.

David Garrison
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 1st day of November, 2024.

SHON T. ERWIN
United States Magistrate Judge

ATTACHMENT A

This warrant applies to information associated with Facebook accounts with Unique Identification Numbers: 100088501780416, which are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California. 100088501780416 was preserved with Facebook case number 9040230 on 10/24/2024.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities from December 1, 2022, to September 17, 2024;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from December 1, 2022, to September 17, 2024, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers;

future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the user from December 1, 2022, to September 17, 2024, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account from December 1, 2022, to September 17, 2024

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2), involving the user ID identified on Attachment A.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.